

## [12] 发明专利申请公开说明书

[21] 申请号 99816949.8

[43] 公开日 2002 年 10 月 9 日

[11] 公开号 CN 1373885A

[22] 申请日 1999.9.13 [21] 申请号 99816949.8

[74] 专利代理机构 中国国际贸易促进委员会专利商标事

[86] 国际申请 PCT/FR99/02176 1999.9.13

务所

[87] 国际公布 WO01/20564 法 2001.3.22

代理人 李德山

[85] 进入国家阶段日期 2002.4.12

[71] 申请人 奥迪卡姆研究开发股份有限公司

地址 法国朗布依埃

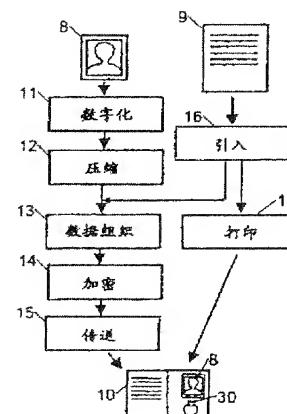
[72] 发明人 杰拉德·米绍

权利要求书 2 页 说明书 5 页 附图页数 1 页

[54] 发明名称 对个人进行安全识别的方法及实现该方法的便携装置

[57] 摘要

本发明涉及一种方法,包含:在赋予个人的薄的柔性纸或塑料识别支撑物(10)上添加关于所述个人的信息;在支撑物(10)上固定一个电子芯片,包含存储器和无触点发送机-接收机,分别用于发送所存储的数据和接收要存储在存储器中的数据;对添加在识别支撑物(10)上的数据进行数字化(11、16)并加密(14);向接收机无触点发送(15)加密的数据并把它们存储在存储器中;以及每次对个人进行识别时,通过读出器接收固定在赋予个人的支撑物(10)上的芯片(30)存储器中存储的数据,对所述数据解密,并将它们与添加在支撑物(10)上的数据进行比较。



# 权 利 要 求 书

---

1. 对个人进行安全识别的方法，包括把所述个人的识别信息添加在一个薄的柔性的支撑物上，如纸、带厚纸背的纸或塑料膜，这一支撑物被分配给所述个人，该方法还包括读出这一信息，所述方法的特点在于它包括：

— 在识别支撑物上固定一个薄的电子芯片（30），其中分别包括存储装置（34）和无触点发送与接收装置（32），从而发送存储的信息和接收要由存储装置存储的信息，

— 对添加到识别支撑物（10）上的信息数字化（11、16），然后对其进行加密（14），

— 把加密的信息无触点发送（15）到接收装置（32）并使所述信息存储在存储装置（34）中，以及

— 在每次对个人进行识别时，通过读取装置（7）接收固定在分配给个人的识别支撑物（10）上的电子芯片（30）的存储装置（34）所存储的信息，对这一信息解密（23），并把这一信息与添加在识别支撑物上的信息进行比较（27）。

2. 根据权利要求1的方法，其特点在于存储在电子芯片（30）中的识别信息包括身份照片（8）和/或指纹的数字化图像，该方法进一步包括：在对所述图像加密（14）之前用图像压缩算法对数字化图像进行处理（12）。

3. 根据权利要求1或2的方法，其特点在于它包括：在对识别信息加密之前，读取由存储装置（34）存储的芯片序列号的阶段，该芯片序列号的存储方式使它不能被改变，这一序列号是唯一的，而且在解密（23）过程中在读这一序列号之前读出由该芯片存储的信息。

4. 根据前述权利要求中任何一个的方法，其特点在于它包括：在识别一个人时，对添加在支撑物上的信息进行数字化（21），并由计算机（1）将这一信息与从该支撑物包含的芯片中导出的信息进行比较。

5. 根据前述权利要求中任何一个的方法，其特点在于它包括：在识别

一个人时，将读出的数据与从数据库中找出的特定个人的一组识别信息进行比较（41），所述信息组是先前存储在数据库中的。

6.根据前述权利要求中任何一个的方法，其特点在于，识别信息是根据预先规定的组织结构存储在芯片（30）上的，需要知道该组织结构才能读出这一信息。

7.用于实现根据前述权利要求之一的方法以识别个人的装置，其特点在于它包括由纸、带厚纸背的纸或塑料膜制成的薄的柔软支撑物，将发送应答器型无触点发送和接收装置（32）与存储装置（34）集成在一起的无触点电子芯片（30），该存储装置与发送和接收装置耦合并在其中存储个人识别信息，该发送和接收装置包括连接装置（35）从而能与传输天线（33）连接，该芯片的厚度极小，从而使它能容纳在支撑物中而不出现任何过大的厚度。

8.根据权利要求 7 的装置，其特征在于芯片（30）为感应型，呈现为线圈形式的传输天线（33）能使读出/写入装置（7）以感应形式向芯片（30）馈送能源，作用于线圈的磁场被调制以便传送信息。

9.根据权利要求 7 或 8 的装置，其特点在于芯片（30）有利地使用几 MHz（兆赫兹）的传输频率，从而使天线（33）能以只包含几圈的线圈形式出现，它们以印刷或丝网工艺印刷方法形成于极薄的柔软支撑物上，以与芯片集成的垫片形式出现的连接装置（35）被焊接在天线的连接端子上，这些连接端子也是由印刷或丝网工艺印刷方法实现的，与天线的连接同时保证了芯片被保持在薄膜（31）上。

10.根据权利要求 7 至 9 之一的装置，其特点在于芯片（30）包括计算装置，如果发送和接收装置（32）接收一个相应的预先确定的密钥，它才授权访问该存储装置（34）的整个单元或一部分。

11.根据权利要求 7 至 10 之一的装置，其特点在于带有芯片（30）和印刷或丝网工艺印刷天线（33）的薄膜（31）被夹在两张普通的或带防护的纸之间。

# 说 明 书

---

## 对个人进行安全识别的方法及 实现该方法的便携装置

### 技术领域

本发明涉及识别个人的一种方法及实现该方法的便携装置。

### 背景技术

它特别是但不仅仅是适用于身份文件的实施例，例如护照和身份证件，它们提供用于识别个人的各种信息要素。这种信息通常包括个人的公民状况（civil status）信息和黑白或彩色身份照片以及可能是人体测量学的信息和手的食指指纹。

身份文件在当前是通过印在纸或厚纸板或增塑纸上生成的。尽管采取了一切预防措施，例如使用特殊纸张，但仍可能使用相对比较便宜的手段以相对比较容易的门路（access）伪造它们。

### 发明内容

本发明的目的是要消除这些缺点。为此目的，本发明提供了一种对个人进行安全识别的方法，它包括在分配给个人的识别支撑物（identification support）上添加有关的识别信息和读这些信息，而这些识别支撑物是薄的、柔性的，或者是用纸做的或是用塑料膜做的。

根据本发明，这一方法的特点在于它包括：——在识别证明件上固定一个薄的电子芯片，其中分别包括无触点存储装置和发送与接收装置，从而发送存储的信息和接收要由存储装置存储的信息。

——对添加到识别支撑物上的信息数字化，然后对其加密。

——把加密的信息发送到接收装置并使所述信息存储在存储装置中，以及

——在每次对个人进行识别时，通过读取装置接收固定在分配给个人的识别支撑物上的电子芯片的存储装置所存储的信息并对这一信息解密，再把这一信息与添加在识别支撑物上的信息进行比较。

这样，本发明的方法使得有可能通过简单地比较芯片中存储的信息和识别支撑物上出现的信息来检验对后者的任何伪造。再有，它利用了先进技术的电子芯片。这样，不可能使用当前的手段，例如印刷手段来产生或伪造它。所以本发明能准确而安全地识别个人。

在电子芯片中存储的识别信息包括身份照片或指纹的数字化图像，这是有好处的，这一图像在加密之前由图像压缩算法加以处理。

这样，对该电子芯片进行有关写和读的访问意味着要知道加密算法和所用图像压缩算法二者。

根据本发明的一个具体特点，该信息是由电子芯片的存储装置根据预先规定的组织结构存储的，需要知道这种组织结构才能读出所存储的信息。

如前所述，本发明还涉及能实现本方法的识别装置，所述装置包括一张薄纸或带厚纸背的纸或增塑纸，一个无触点型电子芯片把发送应答器型发送装置和与所述发送装置耦合的存储装置集成在一处，该发送装置包括连接装置从而与传输天线相连，该芯片的厚度特别小，从而能纳入该支撑物中而不会显出任何显著增加的厚度。

天线为线图形是有利的，它的绕组被丝网工艺（silk-process）印到厚纸片上，通过把连接装置焊接在天线连接端子上使该芯片固定在纸片上。

以这种方式，芯片与传输天线的连接同时保证了芯片在纸片上的固定。

#### 附图说明

下面参考附图描述本发明装置的一个非限定性实施例，这些附图是：

图 1 表示实现本发明方法的系统；

图 2 和图 3 以方框图形式表示本发明方法各阶段的链接；

图 4 表示用于实现本发明方法的芯片。

#### 具体实施方式

本发明的方法使有可能实现一个识别个人的装置，而且是以纸、带厚纸背的纸或塑料片支撑物的形式出现的，在上面附有照片和/或指纹，

并在上面印有所述个人的识别信息。在这一支撑物中装有发送应答器芯片（将在下文中参考图 4 描述），其中包括计算装置（如微处理器心）、存储器以及无触点信息接收与发送装置。

图 1 表示实现本发明方法的系统，包括计算机 1，它与例如键盘的数据输入装置 4，显示屏 3，打印机 6，图像数字化装置 2（如扫描仪），以及例如“无触点”型的发送应答器芯片读出装置 7 相连。

当该系统不仅用于进行安全控制而且需要根据本发明的方法实现一个识别支撑物时，读出装置 7 包含写装置，它能把信息发送到识别支撑物中含有的发送应答器芯片。

图 2 显示根据本发明实现识别装置的各阶段。

本发明的方法使用例如图像 8（例如身份照片和/或指纹）使它可能识别一个人，在第一阶段 11，这一图像首先借助数字化装置 2 被数字化。然后在阶段 12，所得到的数字化图像被压缩处理，它没有明显改变图像质量，使它能存储在容量较小的数字存储器中。通过使用当前的图像压缩技术，有可能性把一张身份照片存储在几百个八位字节上而图像质量只有轻微损失。

与此同时，关于个人的识别信息 9，例如公民状态信息（姓、名、出生日期和地点）以及人体测量学信息（性别、尺码、眼睛颜色），被引入计算机 1（阶段 16），它根据预先建立的顺序（阶段 13）把这一信息与图像信息组合和组织起来，并对它们应用加密算法（阶段 14）。然后将组织好的加密的数据发送到识别支撑物 10 中包含的芯片 30 中，从而把这些数据存储起来。再有，在阶段 11 中引入的信息 9 被打印在支撑物 10 上（阶段 17）。

应该指出，可在阶段 13 之前进行阶段 14，根据所使用的加密算法，这能使得更难于访问由芯片 30 存储的信息。

图 3 显示对带有识别支撑物 10 的个人进行身份控制时进行的操作。

在阶段 22，读出装置 7 请求传送发送应答器芯片 30 中存储的信息。然后这一信息被传送到计算机 1 从而被解密（阶段 23）和分析，从而把识别信息与关于数字化图像的信息分开。该图像信息被解压缩（阶段 24），

然后与识别信息一起显示在显示屏 3 上 (阶段 26)。于是, 进行身份控制的操作员能确认识别支撑物 10 上出现的打印信息和照片清楚地对应于屏幕 3 上显示的信息。

根据本发明的一个具体特性, 所用加密算法是加密密钥型的, 选用的密钥是芯片 30 的序列号, 它是唯一的并被永久存储在它的存储装置中。于是, 加密阶段 14 和解密阶段 23 包含一个首先使用读装置 7 读芯片序列号的操作。

再有, 通过使用扫描仪 2 对加在支撑物 10 上的照片 8 和印在上面的信息进行数字化并由字符识别软件处理该照片和信息 (阶段 21), 有可能性使确认操作自动化。然后, 只需对芯片 30 上读出的信息和从数字化中导出的信息进行比较, 并在显示屏 3 上指出是否已检测到差别, 这便足够了。

与此同时, 可把该信息, 包括从发送应答器芯片 30 中读出的图像信息, 与在计算机 1 上可访问的数据库 41 中存储的关于此人的识别信息进行比较。

在图 4 上, 发送应答器芯片 30 包括存储模块 34 和传送模块 32, 后者由连接装置 35 与天线 33 相连。存储模块和传送模块能被固定在极薄的柔性膜 31 上, 如用聚酯材料制成的塑料膜。这样, 在带有 126kbit 存储容量的发送应答器芯片的情况下, 这两个模块的厚度不超过十分之几个毫米。这一容量足以与要存储的数字图像大小相容, 如果考虑到当前信息压缩技术性能的话。

如前所述, 芯片 30 包括一个微处理器, 用于管理和控制存储器 34 和读、写装置 7 之间的数据传送。这样, 该微处理器能向存储器 34 的整个单元或若干部分分配一个或几个访问密钥, 并在使用错误密钥试图进行访问的次数达到预先确定的一定次数之后完全封锁对该芯片的访问。这样, 未被授权的人便不可能复制该芯片中的内容并把它传送到另一芯片。

芯片 30 的微处理器还被编程以管理冲突, 即在读出器和若干芯片之间同时进行的传送。

再有，在感应芯片的情况下，传输天线 33 以线圈形式出现，使读和/或写装置 7 能通过感应向芯片 30 馈送能量，加到线圈上的磁场被调制从而发送信息。

本发明使用的发送应答器芯片有利地使用几 MHz (兆赫兹) 的传输频率，从而使线圈 33 只包含几圈，它能以简单的印刷或丝网印刷方法在薄膜 31 上形成，以垫片形式出现的连接装置 35 直接放在该芯片的硅基片上，所述垫片被焊接到天线的连接块上，该连接块也是以印刷或丝网印刷实现在薄膜 31 上的，与天线的连接同时保证了芯片被固定在薄膜 31 上。

这些垫片最好以导电胶实现。

此外，有可能把一纸片粘在膜 31 上，从而覆盖和掩蔽芯片 30 和天线 33 的另一表面。

薄膜 31 可以是厚度约  $100 \mu\text{m}$  的聚酯薄膜，从而使该支撑物和芯片构成的单元的厚度不超过  $300 \mu\text{m}$ 。

这样，芯片 30 和薄膜 31 (在其上印刷或以丝网工艺印刷了天线 33) 能以夹心方式装在两张普通的或带防护的纸片之间而不会造成明显过厚，这些纸片承受印刷的识别信息和可能有的身份照片和/或指纹。

应该指出，所使用的传输频率使有可能得到较高的传输流速。结果，读取芯片存储的信息能在几乎是瞬间完成。

# 说 明 书 附 图

